
**State of Alaska Cyber Security &**
**Critical Infrastructure**
**Cyber Advisory**

**March 08, 2016**

*The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**ADVISORY NUMBER:**
SA2016-045

**DATE(S) ISSUED:**
03/08/2016

**SUBJECT:**
Multiple Vulnerabilities in Windows OLE Could Allow for Remote Code Execution (MS16-030)

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Microsoft Windows Object Linking and Embedding (OLE), which could allow for remote code execution. Windows OLE allows an application to link part of a document to another application of a different type for processing. These vulnerabilities exist when Windows OLE fails to properly validate user input. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**
There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- Windows Vista
- Windows Server 2008, 2008 R2 (including Server Core installation)
- Windows 7
- Windows 8.1
- Windows Server 2012, 2012 R2 (including Server Core installation)
- Windows RT 8.1
- Windows 10

**RISK:**
**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**
Multiple vulnerabilities have been discovered in Microsoft Windows Object Linking and Embedding (OLE), which could allow for remote code execution. These vulnerabilities exist when Windows OLE fails to properly validate user input. An attacker could exploit these vulnerabilities by convincing a user to open either a specially crafted file or via a phishing email.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

**REFERENCES:**

**Microsoft:**

https://technet.microsoft.com/en-us/library/security/MS16-030

**CVE:**

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0091

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0092